Opening statement to the Joint Committee on Foreign Affairs and Defence

Chairperson, deputies, and senators, thank you for the invitation to address this committee on the topic of disinformation and hybrid threats.

The Institute for Future Media, Democracy, and Society is a research centre based in Dublin City University (DCU). Through our research and outreach work, we aim to address the major challenges arising from the digital transformation of media, democracy, and society.

Regarding disinformation, DCU coordinates the Ireland hub of the European Digital Media Observatory or EDMO. This network of hubs is part-funded by the EU to support the work of factcheckers, media literacy practitioners, and researchers. Through this and other projects, DCU conducts research on the effectiveness of disinformation countermeasures; supports the implementation of practical measures such as media literacy campaigns; and contributes to Irish and EU policy development; most notably, through our work on the EU Code of Practice on Disinformation and the National Counter Disinformation Strategy.

We do not, however, have expertise in defence, security, or cyber security. In fact, the EU network of EDMO hubs is typically focused on national and public-facing dimensions of disinformation. Nevertheless, I would like to present some insights that I believe may be helpful for the committee to consider.

First, disinformation is a complex concept to define and certain dimensions of it are more prominent in the defence context. The most commonly accepted definition of disinformation is: false information that has been created or shared with the intent to deceive or cause harm. In practice, however, it can be very difficult to ascertain intentions or to trace false claims back to an original source. Moreover, in many scenarios, intentionality matters far less than the harm or outcome that arises. For

example, if false claims lead to widespread distrust in vaccines or undermine the electoral process, the intentionality behind those claims is secondary to the negative public outcomes. For that reason, many of the stakeholders involved in countering disinformation focus their attention on preventing disinformation harms rather than the intentionality of disinformation sources.

Yet, identifying sources and their intentionality matters a great deal in the context of foreign affairs, security, and defence. The concepts of "hostile influence operations", "grey zone techniques", and "hybrid warfare" all presuppose an actor with the intent to cause harm. In other words, the way that people approach the problem in one context doesn't automatically translate into another.

Second, **it is important to avoid assuming a cause and effect relationship between exposure to disinformation and public attitudes**. Popular discussions of disinformation tend to assume that people blindly believe the content they consume. For example, news and research reports often state how many times a disinformation video has been viewed or shared. That just tells us about its popularity; it says nothing about people's attitudes towards the disinformation. In fact, research indicates that people engage with disinformation for all kinds of reasons and that people's acceptance of disinformation is often tied to wider issues including levels of objective knowledge, trust, and ideological bias. In the context of defence and security, it is potentially worth thinking about public vulnerabilities in this context.

Third, there is growing evidence for the effectiveness of "pre-bunking" disinformation. Pre-bunking aims to neutralise the effects of disinformation by warning people about the threat of disinformation and explaining how manipulation tactics work. The underlying idea is to pre-empt the disinformation people are likely to encounter and provide them with the tools to recognise it as manipulation. Given the promise of this approach, researchers are investigating how to integrate "pre-bunking" into fact-checking and media literacy practices. As with all disinformation countermeasures, the challenge, of course, lies in reaching the people who need support.

Fourth, research on disinformation has been hampered by a lack of access to online platforms' data. Currently, independent researchers and policymakers are unable to determine the true scale and impact of online disinformation because they lack access to reliable data. Voluntary EU mechanisms, including the Code of Practice on Disinformation, have failed to deliver relevant insights about the nature of the disinformation that circulates within Member States. In the absence of cooperation from platforms, researchers, journalists and others must invest considerable time and resources to try to understand what is happening online.

Thank you for your time and I am happy to answer any questions you may have.

Dr Eileen Culloty
Coordinator, EDMO Ireland Hub
Deputy Director, DCU Institute for Future Media and Journalism
Assistant Professor, DCU School of Communications